Arc Sight

Arcsight ESM:

- It is a security Information & event management solution.
- It provide's the essentials for security monitoring by leveraging Arc-sight esm superior correlation capability.
- SIEM technology is used in many enterprice's or organisation's to provide real time reporting and long term Analysis of security event's.

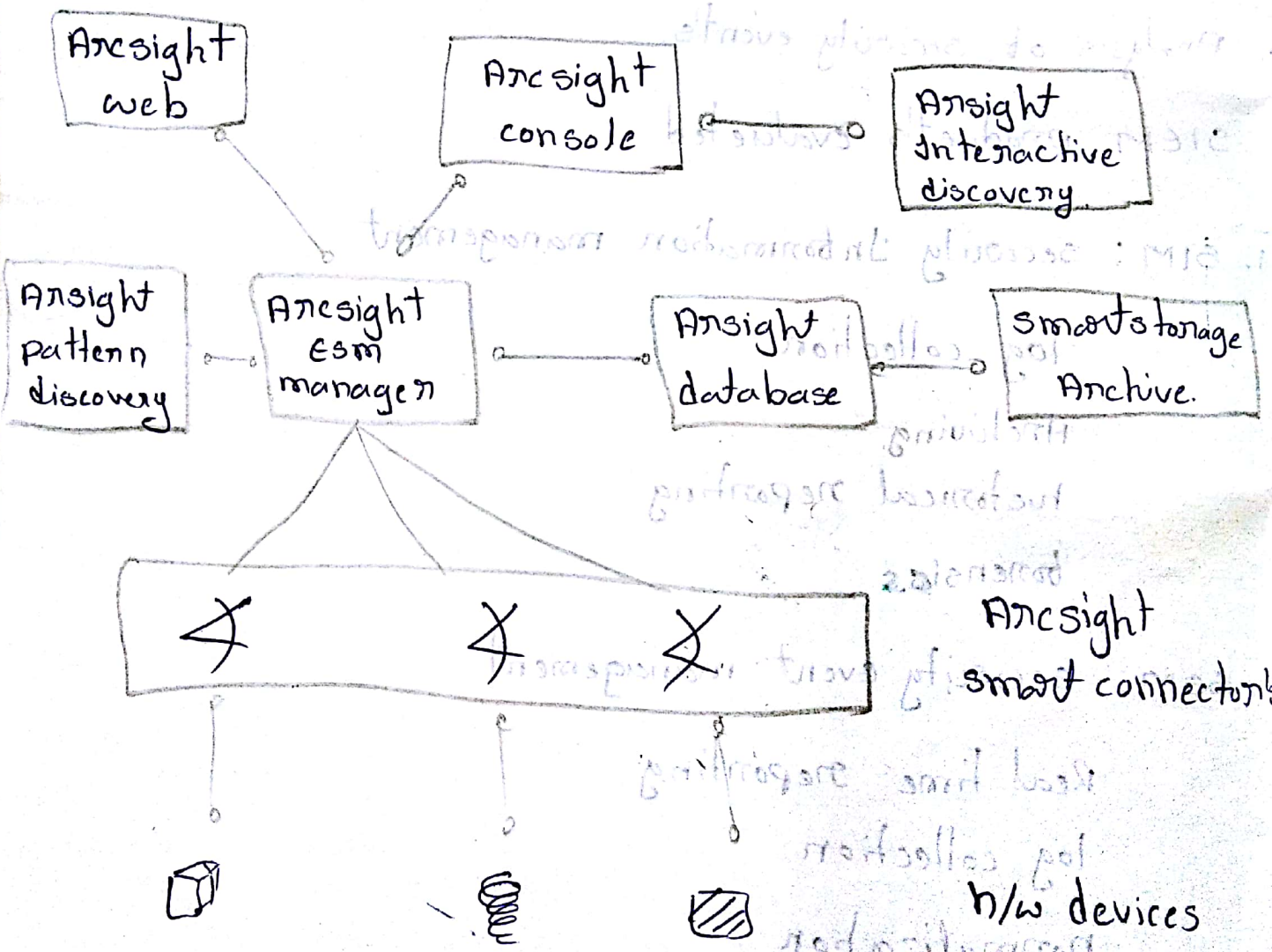
SIEM product's evaluated

1. SIM: security Information management
   - log collection
   - Archiving
   - historical reporting
   - forensics
2. SEM: security event management
   - Real time reporting
   - log collection
   - normalization
   - aggregation
   - correlation.

Scanned by CamScanner

Arc-sight use's:

- pre-build rule's & report's.
- comprehensive event collection
- Esm correlation engine
- User-friendly operator console.
- Fast-deployment & minimal management
- simplified long-term storage.



Multi-tier Architecture to integrate computer security infra structure.

Scanned by CamScanner

Arc sight components:

- Arc sight built on a multi-tier Architecture.
- It consists of
  - * Arc sight smart connector
  - * Arc sight manager.
  - * Arc sight Logger
  - * Arc sight database [CORR Engine]
  - * Arc sight web/console.

smart connector:

- It acts as the Interface b/w the Arc-sight ESM (or) manager and the data source's. That generate's ESM relevant data on your n/w.
- Data collection, normalization, storage etc...
- smart connector collect event raw data from the data source's such as [n/w device's, security device's, servers].
- It's normalize the data into CEF [common event format].
- And smart connector can perform first level of filtering and aggregate event's.

Scanned by CamScanner

- To reduce the volume of events sent to the esm manager.
- which increases esm's efficiency and reduce the event processing time.
- And pass events to the Logger manager after they have been processed.

connector Appliance :

- It is a hardware solution
- the connector appliance centralizes smart connector management.
- smart connector is wizard that install into the servers. that is called connector appliance.

flex connector :-

- esm's flex connector framework is a s/w development kit [SDK] that enables you to create your own smart connector.

Scanned by CamScanner

ESM manager:

- It is the heart of the esm solution
- It is a Java-based server that drive's esm Analysis workflow & services.
- It function's as a server.
- It receive's event data from connector's and correlate's the event's and store's them in the database.
- And also it provide's advanced correlation and reporting capability.

Logger:

- Arc sight logger is an event data storage appliance.
- Logger is a quick searcher and fast report generator.
- Logger receive's event's in [CEF] format from connectors.
- Logger can forward selected events to esm

Scanned by CamScanner

Database :

- The esm database is based on oracle
- Arcsight esm use's storage based on the correlation engine.
  - which receive's event's from manager
  Arcsight esm devide's storage into two catagorie's.
  - System storage
  - Event storage

It store data in 3 way's

1. hot
2. warm
3. cold

User Interface :

- esm provide's two Interface's, Arcsight esm web, esm console. to navigate the feature's and function's of esm.

Arcsightweb :

- Arcsight web Interface having very limit resource's Like active channel's & report's.
- Basically this Interface for client / business team. for checking and download the data.
- It provide's a secure - web - based Interface to the manager.

Scanned by CamScanner

Arcsight console:

- It provide's a user interface to perform administrative tasks on Arc sight.
- It is a tool for building filter's, rule's, report's dashboards & data monitoring.
- It is also the interface for administrating user's and work flow.

It consist's of 3 panel's.

Navigator:

- In Navigator panel we can access all ESM resource's

Viewer:

- The viewer panel is the middle section of the console window. and it display the result's of ESM monitoring & investigating tool.
- It can also display basic HTML, such as HTML-Based report's, reference page's.

Scanned by CamScanner

Inspect/edit:

- It displays details in two cases

when inspecting individual events, during investigation and when editing esm resources.

- edited in the inspect/edit panel, enable's you to view details of an individual events, or to edit values for new(or) existing esm resource's

Data source's:

- Arcsight esm collect's output's from the data source's such as IDS, IPS, switches routers, servers, vulnerability Assistance penetration testing and antivirus etc....

Scanned by CamScanner

collect event data: Data collection:

- Event collection is the process of gathering information from n/w node's. such as n/w device's & security device's & server's.
- These event's are collected by smart connector.
- The data collected is log data generated by the different types of sources on your network.

Normalization:

- smart connector collect's the raw data generated by different type's of device's such as n/w, security, servers.
- All format's are different, it's difficult to understand.
- Because n/w are heterogeneous environment's.
- each device has a different logging format & reporting mechanism.
- so it's very difficult to understand or extract without normalization.
- so that smart connector convert that raw events into CEF format.

Scanned by CamScanner

Aggregation:

Aggregation consolidate's event's with matching value's into a single aggregated event.

- which reduce the number of event's the manager must evaluate.
- which increase esm efficiency and reduce event processing.
- connector aggriegation merge's event's with matching value's into a single aggregated event.

correlation:

- It is a process that discover's the relation b/w event's.
- Inverse the significance of those relationship prioritize them & then provide's a framework for taking action.
- It is a proprietary data storage & retrieval frame work.
- that receive's and process event's at high rate's. & perform high speed search's.
- A correlation is a s/w application, that programmatically understands relationship's.

Scanned by CamScanner

Annotation's:

- Annotation's are used to assign that event to a particular user (or) usergroup's to escalate.
- Annotation's are light-weight workflow tool's, we can use to track and escalate event's through our workflow.
- Annotation's is a field in the esm event schema that enable's you to flag an individual event or group of related event's for follow-up.

workflow:

- The workflow framework provide's a customizable structure of escalation level's.
- To ensure that event's of interest are escalated to the right people. in the right time frame.
- This enable's member's of your team to perform immidiate investigation's, make informed decision's and take appropriate.

Scanned by CamScanner

Monitoring:

- Esm provides a variety of flexible monitoring tools.
- That enable's you to investigate and remediate potential threats. before they can damage your network.

Analysis:

- Esm provide's an array of investigative tool's.
- That enable member of your team to drill down into an event and perform function's, such as: Ns lookup, ping, portinfo, Traceroute, Web search and who is...

Reporting:

- Esm reporting & trending tool's can be used to crea versatile, multi-element Report.
- That can focus on narrow topic's.
- They can also be used to report general system status either manually (or) automatically on regular schedule.

Scanned by CamScanner

Active-channel:

- Active channel is a collection of real time or historical event's defined by parameter's.
- Active channel's can be configured by two option parameter's.
  - continuously evalution time parameter:
    - real time view of event's being sent from connector's into manager.
    - it's good for real time event's view.
  - Evalution time parameter:
    - view event's saved to a database.
    - During a specific time range.
    - it's good for historical Analysis.

* There are three type's of active channel's that display's different type's of data.
  - Live channel's: Display continuously refreshed Live event data.
  - Rule's channel's: display replay event's for testing rule's.

Scanned by CamScanner

- Resource channels:

Display the status of certain resources, such as the assets in your n/w model and open cases.

Scanned by CamScanner

Filters:

- Filters are set of conditions, that focus on particular event attributes.
- This focus also reduce the number of events that are processed by the system.
- Filters are applied in many places in the event like cycle of smart connector, the manager & correlation engine.
- Filters are also used in monitoring, analysing and reporting.

* Filters applied at the smart connector select only events, that match the conditions And
  - These events are forward to the manager, non matching events are not forward to the manager.
* Filters are applied at the manager includes.
  only the events that will be processed based on specific conditions.
  - All other events won't be processed but will be written to the db.

Scanned by CamScanner

- Filter condition statements are constructed using ESM's boolean logic editor. and also referred to as the common condition editor [CCE].
- ESM filter's come in two major forms:
  - * Named condition
  - * Unnamed condition

* Named condition:
- A filter resource is a named object that can be referred by other resource's and smart connector.
- Filter resource's are reusable, and can be transported among manager's.
- If we want to use the same condition in multiple place's, create a filter resource's. we can then refer to in rule's, report's, data monitor's & active channel's.
  - * Named condition's are reusable.

* Unnamed condition:
- Unnamed condition's reside within another resource's.
- These are used to specific condition's that are applied Locally by that resource only.
  - * These are not reusable.

Scanned by CamScanner

Rule's:

- ESM rule is a programmed procedure that evaluate's incoming event's bon specific condition's and pattern's
- when a match is found, can initiate action's in response.
- Rule's are the centerpiece of the esm correlation engine.
- ESM rule's are similar to [IDS] rule's.
- Rule's are constructed using aggregation & boolean pattern's matching to evaluate object's.

* There are two type's of rule's available in ESM:

both simple and join rule's, can apply aggregation.

Simple:

- simple rule's are triggered when event's match one set of condition's.

Join:

- Join rule's are triggred by event's that match two or more set of condition's.

Join means to connect event's from different n/w node's in order to understand attribute's they may have in common.

Scanned by CamScanner

Reports:

- Reports are captured views or summaries of data, that can be printed displayed in the console or in the web interface.

The data that can be printed or viewed in the Arcsight console or management console viewer in a variety of formats. such as PDF, Html, XLS, RTF...

- A report binds one or more queries/trends. with a report templates.
- query can collect data from trends, session lists, active lists in addition to reporting on event data.
- Reports can also summarize* internal esm data from cases, notifications and assets.
- Reports can optionally be focused on subdivision of data [focused reports]
- Reports and focused reports can be scheduled, and their output saved as archived reports.
- once a report is created, you can run it - manually, schedule it to run automatically at regular intervals.

Scanned by CamScanner

- ~~A Report is one or more trends/queries bound to a report template.~~

~~- queries can collect data from trends, active~~

Queries:

- A query is an esm resource that defines the parameters of data you want to gather from an esm-data source. & reporting events to esm.
- The results of the query then become the basis for one or more report or trend.
- As a data source, queries can use the Arc-sight db of events, assets, cases, notifications, active lists, session lists, or data gathered from a trend.
- In a query, you select data fields you want to report on, specify any ~~age~~ additional functions you want to run on them [such as sum, avg, --] and any sort or group by conditions you want to add.
- one query can be referenced by many reports and Trends.
- The standard reports that esm comes with all reference queries.

Scanned by CamScanner

Trends:

- A trend is an Azure resource's that defines how and over what time period data will be aggregated and evaluated by trends.
- A trend executes a specified query on a defined schedule and time duration.
- Trend is always based on a query.
- A trend results are stored in a trend table in the Azure-sight database, and are themselves queryable.

*: query time taken & Trends give quick output.

Scanned by CamScanner

cases:

- cases are built-in trouble-ticket system, designed to track individual or multiple related events and export event data to third party products.
- cases are intended for use with individual or multiple related events.
- cases are designed to stand alone within ESM or integrate with a third-party case management system, such as BMC remedy)
- A case is a container for information about a specific incident, usually with one or more events attached, (that is used to track, investigate, and resolve events of interest.)
- (when events of concern (కేసులు) occur, you can create cases & assign them to analysit. so analyst will investigate and resolve it.)

Scanned by CamScanner

ESM event life cycle

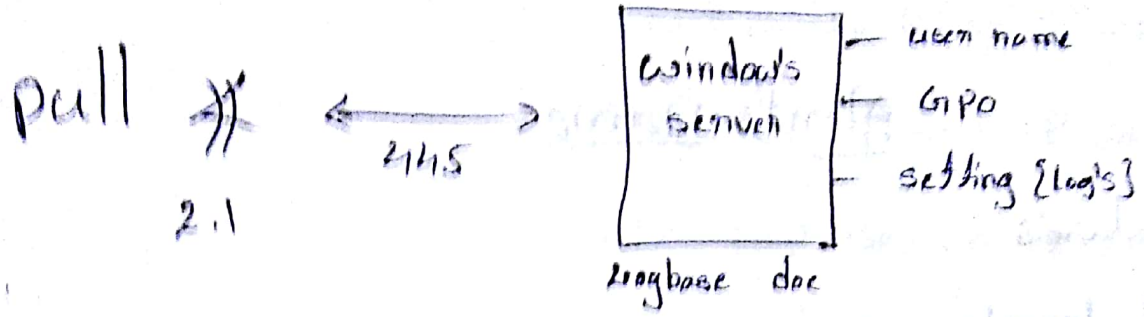
It is classified into 7 case's.

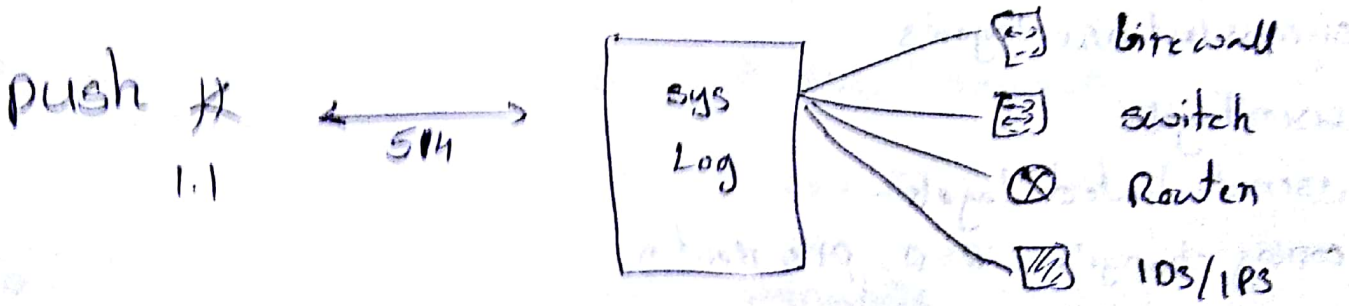
1. Data collection & event process
2. Event priority evalution & Asset model lookup
3. Correlation
4. monitoring & Investigation
5. workblow.
6. Incident analysis & reporting
7. storage & Archive..

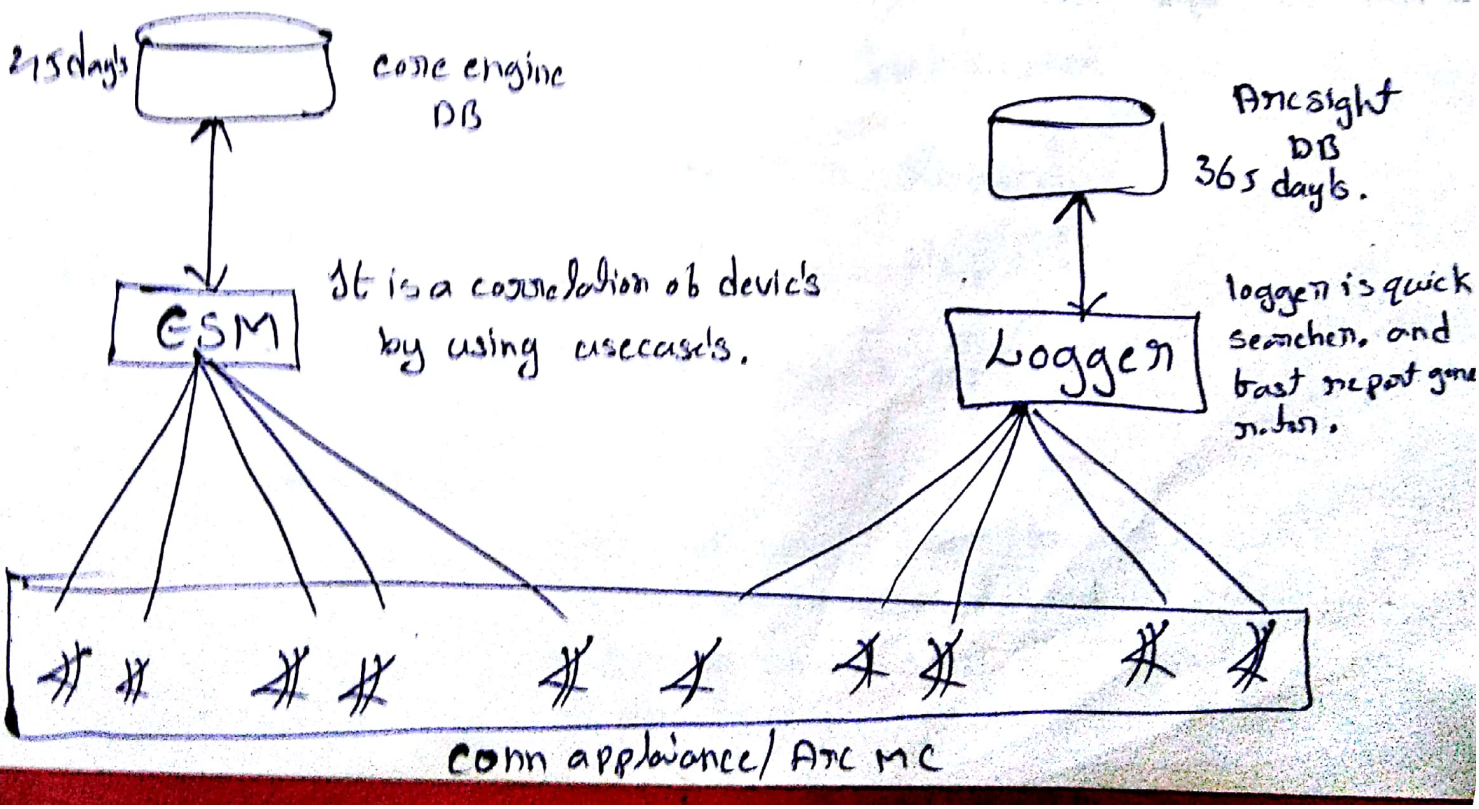
Scanned by CamScanner

Device onboarding issue's

- Firewall port issue
- Device setting issue
- Authentication issue.






215 days
core engine DB
ESM
It is a correlation of devices by using usecases.
Arcsight DB 365 days.
Loggen
loggen is quick searchen. and fast report gene rator.
Conn appliance/ Arc MC

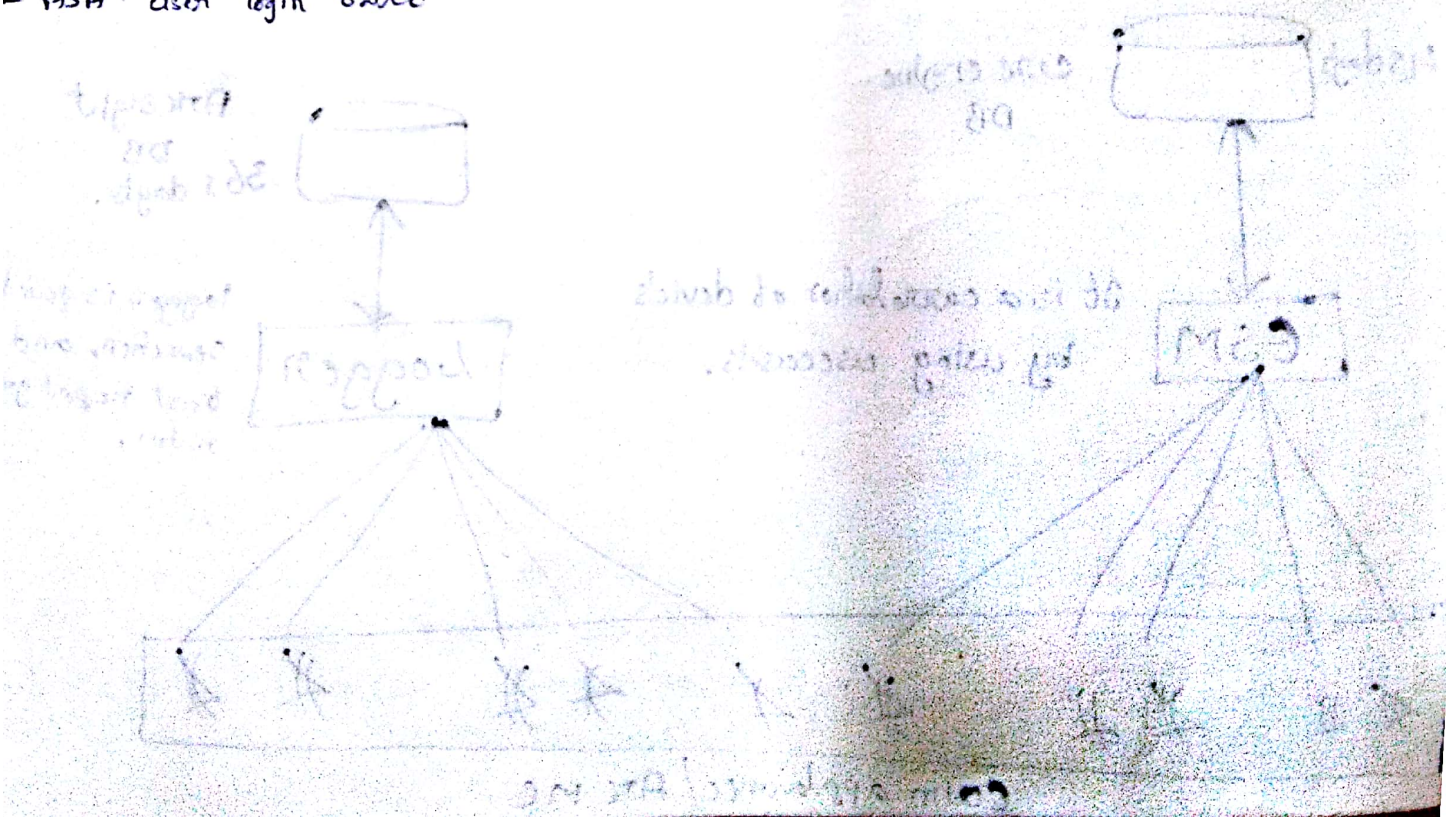
Scanned by CamScanner

EPS [Event per second]: - per day we will get

- Number of events generated by a single device or group of devices.
- Naturally it is used to calculate total number of event's sends to Arcsight.

Alent's names

- Logon failure's
- successfull logon's.
- successfull h/w logon's.
- user logoff
- user initiated logoff
- config change's, ASA, PIX Router
- ASA user login failed



Scanned by CamScanner

Daily Reports [xyz]

S.No	D.R
1	ASA - config change's
2	PIX - config change's
3	Router config change's
4	checkpoint - policy change's.
5	ASA - Top Denied IP report's
6	PIX - Top Denied IP report's
7	checkpoint - Top10 Denied IP report's
8	Firewall Event summary report
9	Event count
10	IPS signature report
11	Daily dashboard
12	Solaris Report
13	Linux Report
14	window's Report

- Linux:
  - SU [switch user] login failure's
  - user added & user deleted
  - service start & stop
  - shut down
  - Reboot

Scanned by CamScanner

Bank, solaris, windows, Linux - Reports.

parameter name	parameter value
Time zone	Asia/calcutta
start	May
end	May

- password changed - Time Event type username Host address
- user created - Time Event type Host address Host name username
- user deleted - End time name destination address Destination host name destination username
- ftpd - failed login - Time Name source address Destination address Destination host name service name
- service stop - Time name Device address Device host name Device process name source address destination address
- su failed - Time name source username Destination user name Destination address source address Device address.
- sys, shut down - Time of the event Event Host IP Hostname Device process name source address destination address.

Event's - action taken Report 30-May-16

Events count changes approved by IT Team comments.

action taken by signature.

Scanned by CamScanner

Bank – ASA, PIX, Router, check point. config changes.

parameter name	parameter value
Time zone	Asia/calcutta.
start_time	may 30 2016, 00:00:00
end – time	may 31 2016, 00:00:00

Time	Name	link name	Device address	Destination host name	source user name

firewall change's – Action taken report 30-may-16

Device address	Rule base change's requested by SOC	Rule base change's approved by ISO	status

Action taken by :

signature :

Bank – PIX, ASA, check point – CORE DIR – TOP 10

source address	Destination address	name	count

Event collection status report – event count

Device host name	Device address	number of event's received	owner/ process
Firewall's			
⋮			
Router, windows solaris, Linux.			

Scanned by CamScanner

- event collection status reports, number of events received based on device hostname or device address.

- config change's reports such as cisco ASA, PIX, Router, check-point's, with the fields are Time, name, file name, device address, Device host name, source username.

- Top-10 Deny's reports in cisco ASA, PIX, checkpoint, router, with the field's are source address, destination address, name, count.

- window's, Linux, solaris servers reports, such as password-change's, user created, user deleted, ftpd failed login's, any service stop's, su failed, sw, c, shut down's with the field's are time, name, source username, destination username, destination address, source address, Device address.

Scanned by CamScanner

Trouble shooting

ping: packet Internet gopher -t for continue.
[Friend like Traceroute extra]

- ping uses to check the n/w connectivity
- Allows you to send a signal to another Device, on the n/w, to see if it is Active

How does it works:

uses the ICMP [Internet control message protocol] to send out an - "echo request" to the destination device and gets back an echo response. If the device you are trying to reach of Intact active.

Trace root:

- It's a computer n/w tool used to determine the route taken by packets. across an IP packets.
- Trace root let you see the step by step route a packet takes to the destination you specify.
- so if you send a packet to google.com. before the packet actually reaches google.com server.
- it will go through many different routers before it finally reach's gole.com.

- NSLookup:

Server and host identification

Scanned by CamScanner

1 Network team's

2 server team's ← windows
unix/Linux.
IBM/AIX.

3 security team's:

1. VAPT [vulnerability Assistance & penitration testing]
2. phishing team
3. Antivirus team.
4. Malware Analysis team
5. Threat Intiligence team
6. soc team ✓
7. DLP ✓

we are "soc" team [security operation center]

SIEM - Tools

- HP Arc sight ✓
- IBM Q Radar
- EMC² RSA Envision
- Intel Macabbe nitro
- splunk

Scanned by CamScanner

IP Address classes: IP version 4

class	1st octal decimal range	n/w Host id	Default subnet mask	Total Address in class
A	1 - 126	N H H H	255.0.0.0	2,147,483,648
B	128 - 191	N N H H	255.255.0.0	1,073,741,824
C	192 - 223	N N N H	255.255.255.0	536,870,912
D	224 - 239	⟶ Multicasting ⟵		268,435,456
E	240 - 254	⟶ Defence & Research ⟵		268,435,456

Note:

class A address 127.0.0.0 to 127.255.255.255 cannot be used, and it is reserved for loopback and diagnostic functions.

IP address: It's given to a computer in the n/w for identification and communication.

- It's a logical address.

Special IP address:

0.0.0.0 ⟶ Global n/w id

255.255.255.255 ⟶ Universal broad cast ID

127.0.0.0 to 127.255.255.255 ⟶ Loop back range

169.254.0.0 to 169.255.255.255 ⟶ APIPA range.

(Automatic private IP Addressing)

Scanned by CamScanner

private ip	public ip
- used with LAN (or) within the organization	used on public wire [internet]
- not recognized on internet	Recognized on internet
- given by administrator	given by the internet service provider [ISP] [from IANA]
- Unique within the wire organization	globally unique.
- free	pay to service provider
- unregistered IPs	Registered IPs.

private IPs :

class A	10.0.0.1	to 10.255.255.255
class B	172.16.0.1	to 172.31.255.255
class C	192.168.0.1	to 192.168.255.255

Scanned by CamScanner

what is n/w?

- It is an interconnection device

- Networking is the communication b/w interconnected device.

protocols:

- protocols are rules that governs how devices communicate & share information across a n/w.

Ex: IP - Internet protocols

HTTP -

HTTPS -

SMTP - simple mail transfer protocol.

LAN:

- A LAN is generally a high speed n/w that covers a small geographic area, usually contained within a singl building or campus.

- It's is usually under the administrative controll of single organization.

- Ethernet is the most common LAN technology

- users can communicate with each other and tran ter data b/w workstations very easily.

Scanned by CamScanner

WAN:

- It's a n/w that covers large geographical locations, usually to connect multiple LAN's.

VPN:

- It allows our information to be securely sent across a public (Internet) unsecure n/w.
- It enables users to send and recive data. securely.
- Packets with a private destination address are ignored by all public routers.
- Two private n/w cannot communicate via the public Internet unless they use an IP tunnel or "VPN".
- when one private n/w wants to send a packet to another private n/w, the first private n/w encapsulates the packet in a protocol layer, so that the packet can travell through the public n/w.
- Then the packet travells through the public n/w. when the packet reaches the other private n/w, it's protocol layer is removed, and packet travells to it's destination.

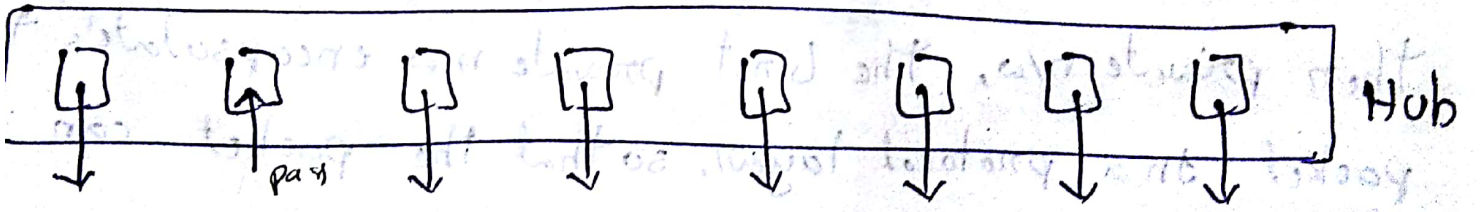
Scanned by CamScanner

Network Device's

* Hubs
* Repeater's
* Bridge's
* switches
* Routers.

* Hubs:

- A hub Interconnect's two or more workstation's into a Local area network [LAN].
- It's a layer1 device, simple Interconnecting device. when a computer on any one of the 8 port's transmit data, this is replicated and send out to the other 7 port's.



Repeater's:

works similar to hub's, additionally boost's & Regenerate's the signal's.

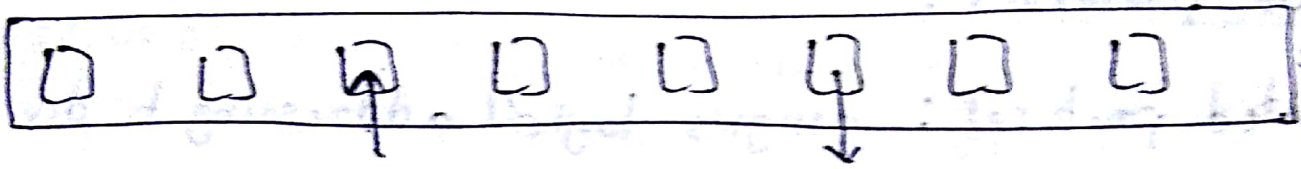
Pass Incomming traffic to all other connected port's.

They don't perform data filtering.

Scanned by CamScanner

switch :

- It's layer 2 device.
- unlike hubs, it reads source MAC address and destration MAC address.
- Look into MAC table & find the outgoing port information & send to that port.
- It work's based on MAC address.
- It maintain's mac address table.



switch MAC-address table

Vlan	MAC address	Type	Port's
1	0000.aa67.b4c5	DYNAMIC	Fa0/4
1	0000.aa70.d9b9	"	ba0/7
1	0001.e641.96cd	"	ba0/2

Scanned by CamScanner

Router:

- It's a layer3 device.
- It works based on the IP address.
- It can make intelligent decession about how to choose best path through or to a n/w.
- Router interconnects two n/w.
- It can maintain routing table.

Two protocols:

- Routed protocol: assigns logical addressing to devices and routes packets b/w n/w. Ex: include IP & IPX
- Routing protocol: dynamically builds the information in routing tables. Ex: includes RIP, EIGRP, and ospf.

Route types:

- static routes: where to send traffic created by a administrator.
- Dynamic routes: DHCP uses a routing protocol to determine the best path. with dynamic routes, routers communicate with each other and exchange routing information.

Scanned by CamScanner

Routing:

Routing is the process of forwarding a packet from one n/w to another n/w. based on the n/w layer header. Routers build routing tables to perform forwarding decessions.

Destination	Netmask	Gateway	Interface	metric
207.22.36.0	255.255.255.0	195.209.285.1	195.209.225.0	1
207.22.36.0	255.255.255.0	195.209.285.10	195.209.225.50	2
194.0.0.0	255.0.0.0	193.11.17.44	193.11.117.1	8

ACL:

- It's a layer 3 [n/w] security which controll's blow of traffic from one router to another router.
- It's also called a packet filtering firewall.
- ACL is used to block traffic based on ip address and transport layer port number's.
- It seperate's ACL's for Interface, Inbound & outbound traffic.
- Generally ACL implements on distribution layer - Router's.
  - standard ACL
  - Extended ACL
  - named ACL

Scanned by CamScanner

Security device's

* firewall's
* IDS
* IPS

* firewall's :

- firewall is a n/w security device, either hardware / software.
- It's provide's the secure connectivity b/w n/w.
- It controll's incoming and outgoing n/w traffic based on the set of rule's.
- It works based on the IP address & port number's.

can:

- firewall can block invalid packet's & filter's the traffic based on a defined set of filter's.

can't:

- firewall's are unable to block virus & malicious code.
- prevent attacks by malicious users allready behind the firewall.
- And is unable to protect data after it passes out of or into the private n/w.

Scanned by CamScanner

different types of firewalls:

- packet filter router fw
- application-layer fw
- stateful fw
- proxy firewall

proxy:

- Doesn't allow client to directly connect to the server.
- maintains complet connection state & sequencing thrgh 2 connections.

client to proxy

proxy to server.

Scanned by CamScanner

IDS & IPS:

- These are seccority device's.
- These are specially designed to monitor all inbou. & outbound n/w activity.
- It's woorks based on the signatures's.

IDS:

- A device that analyzes whole packet, both header and payload. looking boor known event's.
- when a known event is detected a log message is generated detailing the event.

IPS:

- A device that analyzes whole packet's, both header and payload, looking boor know event's.
- when a know event is detected the packet is rejected.

Scanned by CamScanner

Port numbers

Port number (0 - 10^3)	service's
20	FTP data
21	FTP control
22	SSH
23	Telnet
25	SMTP
37	Time
53	DNS
67	DHCP
80	HTTP
~~Delete~~	
109	POP②
110	POP③
115	SFTP
118	SQL services
156	SQL server
161	SNMP [simple n/w management protocol]
179	BGP [borden gate way]
2443	HTTPS
445, 137, 139	microsoft - DS [SMB]
546	DHCP client V6
547	DHCP server V6

Scanned by CamScanner

The range of port numbers are 0-65535 for both TCP & UDP

- The combination of the ip address and port numbers [identifying both the host & service] is referred to as a "socket" and is written out as follows.

"192.168.60.125 : 443"

Note: The colon seperating the IP address [192.168.60.125] from the port number [443].

The first 1024 port's [0-1023] have been reserved for widley-used services and recognized as "well known port's". Below is a table of several common TCP/UDP port's.

Port number	Transport protocol	Application
20, 21	TCP	FTP
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP/TCP	DNS
80	TCP	HTTP
666	TCP	Doom

Scanned by CamScanner

ports ranging from 1024-49151 are referred to as registered ports, and are allocated by the IANA upon request.

- ports ranging from 49152-65535 cannot be registered and are considered dynamic.

A client initiating a connection will randomly choose a port in this range as it's source port.
[for some os, the dynamic range starts at 1024 and higher].

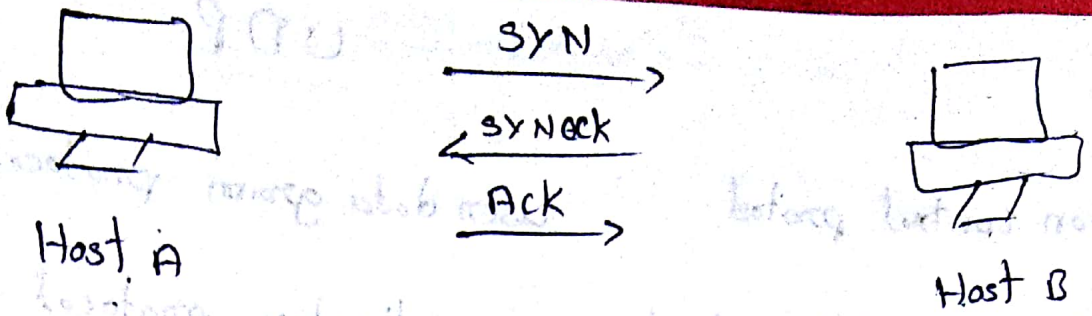
RDP - 3389
Oracle - 1521

TCP	UDP
- Transmission control protod	user data gram protocal
- It's connection oriented protocol	connectionless protocol
- TCP is more reliable than UDP	UDP is more faster than TCP for data sending.
- header size of TCP is 20 byte's	UDP is 8 byte's.
- TCP has acknowledment segments	no Acknowledgement.
- TCP give's guarantee that the order of data at receiving end is same as on sending end	UDP has no such guarantee.

TCP connection establishing: 3 way hand shake

- TCP is a connection oriented, so it's requires connection establishment before data transfer begin's.
- for a connection to be established, two host's must synchronize on each other's "Initial sequence number" (ISN)
- ISN's are actually large random numbers choosen by host.

Scanned by CamScanner



- Host A sends a "syn" message to Host B to initiate a connection.
- Host B receives "syn" and send's a synchronous Acknowledgement to Host A
- Host A receives syn-Ack. and send's Acknowledge.
- Host B receives Ack.

"TCP connection is established".

The range of port no is 0-65535 bus both TCP & UDP

Risk:

- Risk is the intersection of Asset's, Threat's and vulnerabilities.
- The protection for loss, damage or destruction of an asset, as a result of a threat exploiting vulnerability.

Threat:

- In the n/w security, Threat's are potential's for vulnerabilities, to turn into attacks on computer system.
- Threat's can leads to attacks on a computer system.
- Threat's are something that may or maynot happen.
- Threat's can include everything from virus, worm's, Trojan's, backdoor's, to outright attacks from hacker's.

Vulnerability:

- In a computer security, vulnerability is nothing but a weakness or flaw, which allow's an attacker to reduce a system's information assurance.
- Vulnerability is the intersection of three elements a system suspectability or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

Scanned by CamScanner

Attacks

what is attack?

- In a computer n/w, an attack is any attempt, to destroy, expose, alter, disable, steal and gain unathorized access. to or make unathorized use of an asset.

Asset:

- An asset is what we are trying to protect.

Hackers/crackers: Attackers:

- A person, whose trying to gain the unathorized access.

Back doors:

- It's also called as a "trapdoor".
- It's a method of gaining access to a program, online services, or an entire computer system.
- Allows to execute privilized operations on the affected machine.

Victim:

- Targeted machine in an exploit.

Zombie:

- A machine used for attack (or) A compromised machine

Scanned by CamScanner

Botnet attack:

- It's a collection of compromised computer's [zombie]
- usually installed via virus, worm's, Trojan's or backdoors
- A botnet originator [bot header] can controll the group remotly.

zero day attack:

- The zero day attacks occur's on the same day. ex: a weakness is discovered in a software.
- At that point it's exploit by hacker's, before the vendor become's aware and hurry to fix it.

Scanned by CamScanner

Common exploiting technique's:

Password cracking method's:

Brute force attack:

- It's one of the most common method to crack the passwords.
- This attack is basically Trail & error method, usually to find the legitimate authentication credential's.
- This attack's sometime's take's longer, but it's success rate is very heigher.
- In order to gain the password authentication's, attackers can use password guessing tool's & script's.

  such as cainaable, hashcat, rainbow crack et- - - -

packet sniffers:

- packet sniffing is the act of capturing packet's of data flowing across a computer n/w.
- sniffers are mainly used to capture the traffic b/w the networks.
- In order to find username, password's, confidential information

Scanned by CamScanner

phishing (or) spoofing attack:

- phishing (or) spoofing attack's are used to steal the consumer's personal identity data & financial account credential's.
- Hacker's use "spoofed" email's to gain financial data such as account number's, username's, password's credit card number's.

- spoofing is the creation of TCP/IP packet, using somebody's IP address. and send a packet to a victim computer with an ip address, indicating that the message is coming from trusted host.

social engineering:

- The most prevelent type of social engineering attacks are conducted by phone.

scanning: ⊙

- An attacker generally want's to connect to a host to gather information about open port's, os, or application's on the host.

Scanned by CamScanner

Man In the middle [MITM] attack:

- This is also called as a connection hijacking.
- These kind's of attacks Intereptis a legitimate communication b/w two system's.
- To control the blow of communication, and alter the Information's sent by one of the original participant's. without their knowledge.

For example In an http transaction, the target is the TCP connection b/w client & server.

- the attacker splits the original TCP connection into 2 new connection's, by using different technology's
- one b/w client & attacker and another one is attacker & server.

once the TCP connection Interepted, the attacker acts as a proxy. being able to Insert, read & modify the data In the Intercepted communication

Scanned by CamScanner

Bubber overblow attack:

- Bubber overblow occur's anytime. when a program or process write's more information into the bubber. than the space, it has allocated in the memory.
- This allows an attacker to overwrite data that control's the program execution path & hijacking the control of the program.

session hijacking:

- It's also known as the TCP session hijacking & cookie hijacking is the exploitation of a valid computer session. (or) These kind's of attack's are used to exploit the valid computer session's.
- To gain unathorized access to information or service in a computer system.
- The session hijacking occur's when a session token is sent to a client browser from the web server.

Scanned by CamScanner

SQL Injuction

- sql injuction is an attack.
- sql injuction is one of the most commonly exploited web application vulnarability. at the databas layar.
- By using sql injuction method attackers can create, read, modify or delete's sensitive data.
- The vulnarability is one of the oldest, most prevelent and most dangerous of web application vulnarability.
- It refers to an injuction attack, wherein an attacker can execute malicious sql statement's. That controll's the web application's database servers. [RDBMS].

Scanned by CamScanner

malware attack's

- malware is nothing but a "malicious software" or "malicious code"
- this is a s/w that is specially designed to gain access or damage a computer without knowledge of the owner's.
- there are various types of malware's.

- virus:
- It's a malicious software or code.
- the virus code is injucted into the executable files whenever we run the program, it spread itself.
- these types of malicious applications can spread from one computer to another computer. leaving infections as it travells.
- But it can't infect your computer unless we run the malicious program.
- these types of virus's can't be spread without human action.
- It can damage our hardware, software, or file's.

Scanned by CamScanner

Worm's:

- Worm's are another category of malicious software's.
- It's self replicating and self propagating.
- A worm can spread from system to system automatically without a carrier program.
- Rather than your computer sending out a single worm, it could send out hundred's or thousands of copy of it self
- Both virus & worm's execute's without the knowledge or desire of the end user.

Trojan horse:

- Trojan horse is a program
- that pretends to be a useful s/w, but actually it install's malicious (or) damaging s/w behind the scenes.
- Trojan's can be use to take over a remote.
- But unlike viruses, worm's, it cannot self replicate and cannot re produce, by infecting other file's.

Scanned by CamScanner

Spyware:

- Spyware is a s/w
- that aim's to gathering the information about a user activity without their knowledge.
- and Transmit that information in the background to someone else.
- spyware can also gather information about e-mail's address, and even password's & credit card number's.
- It cannot reproduce by infecting other file's, and nor do they self-replicate.

Adware:

- Adware is a s/w application, that display's or download's advertisement's to a computer.
- Adware is a typically bundled and download with other s/w's.
- If you don't carefully read the term's & condition's of the original program's, you can easily consent to inviting adware on your computer.
- when typing into a search engine, your web request's may be redirected to other advertisemet website's.
- Affect's performance of your computer & the information.

Scanned by CamScanner

DOS:

- when a single host attacks [An attacker can send 100's of connection from one computer to another host [web server]]
- An attacker is going to send a lot of connection's to the victim computer. such as TCP, UDP, ICMP connection's.
- To overload the system memory & increase the CPU usage and bandwidth. It cause's server become overloaded & stop working.
- whenever somebody want's to connect the web server it's got down. due to the overloading.

DDOS:

- when a multiple host attack simultaniously.
- The path of execution method is the same as Dos But there is a key difference.
- Instead of using one computer, attacker can use multiple computer's. 100, 1000's.
- one attacker can controll these many computer's

Scanned by CamScanner

Ransomware attack:

- It's a malware that install's covertly on a victim - computer.
- for data kidnaping, an exploit, in which the attaker encrypt's the victim's data.
- And demands payment for the decryption key.

- Ransomeware malware program's may also be called a cryptovirus, crypto Trojan's or crypto worm.
- more advanced malware's encrypt's the victim's file's, making them inaccessible, and demand's a ransom payment to decrypt them.

* After a victim descover's he cannot open a file, he receive's an email 'ransome note' demanding a relatively small amount of money in exchange for a private key.

* The attaker's warn's that, if the ransom is not paid by a certain date, the private key will be destroyed. and the data will be lost forever.

Scanned by CamScanner

protocol's:

HTTP: Hypertext transfer protocol (80)

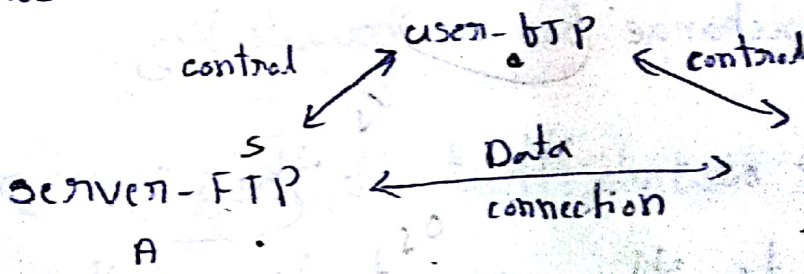
- set of rule's for transfering file's (text, graphic, image's, sound, video,-) on the world wide web.
- As soon a web user open's their web browser, the user is indirectly making use of HTTP,
- It's a application layer protocol.

HTTPS: Hypertext transfer protocol secure (443)

- HTTPS is the secure version of HTTP,
- It's encrypt's the all communication b/w our browser & the website's.
- It's often used to protect highly confidential online transaction's, like online banking and online shoping order form's.

FTP: file transfer protocol (20, 21)

- It's a standard n/w protocol, used to transfer file's from one host to another on the TCP protocol.



- It's the most common protocol for moving file's from one location to another.

SFTP: secure file transfer protocol

- It's a way for transfering file's b/w machine's over a secure and encrypted connection.

Scanned by CamScanner

ICMP: Internet control message protocol

- It's an error reporting protocol
- Routers use to generate error message, to the source IP address, when n/w problems prevent delivery of IP packets.

Telnet: Terminal network. (23)

- It's an application layer protocol for virtual terminal service
- It's used to communication b/w client & server.
- The connection is "n/w virtual terminal", under the situation.

DHCP: Dynamic host configuration protocol 67

- It's an application layer protocol.
- used to dynamically distributing the n/w configuration protocol such as IP address.
- with DHCP computer's request IP address and n/w parameters automatically from a DHCP server.

SMTP: simple mail transfer protocol. (25)

- It's the standard protocol for sending email's across the n/w

DNS: Domain name system. (53)

- It's translate's the domain & Hostname's into IP address.

SNMP: simple n/w management protocol (161)

- It's a standard protocol that collecting and organising information about managed device on IP n/w.
- This device that [illegible]

Scanned by CamScanner

TLS — Layer 6 - Transport layer security.

- It's provides the secure communication on the Internet, such things as e-mail, Internet banking, and other data transfer's.

Scanned by CamScanner